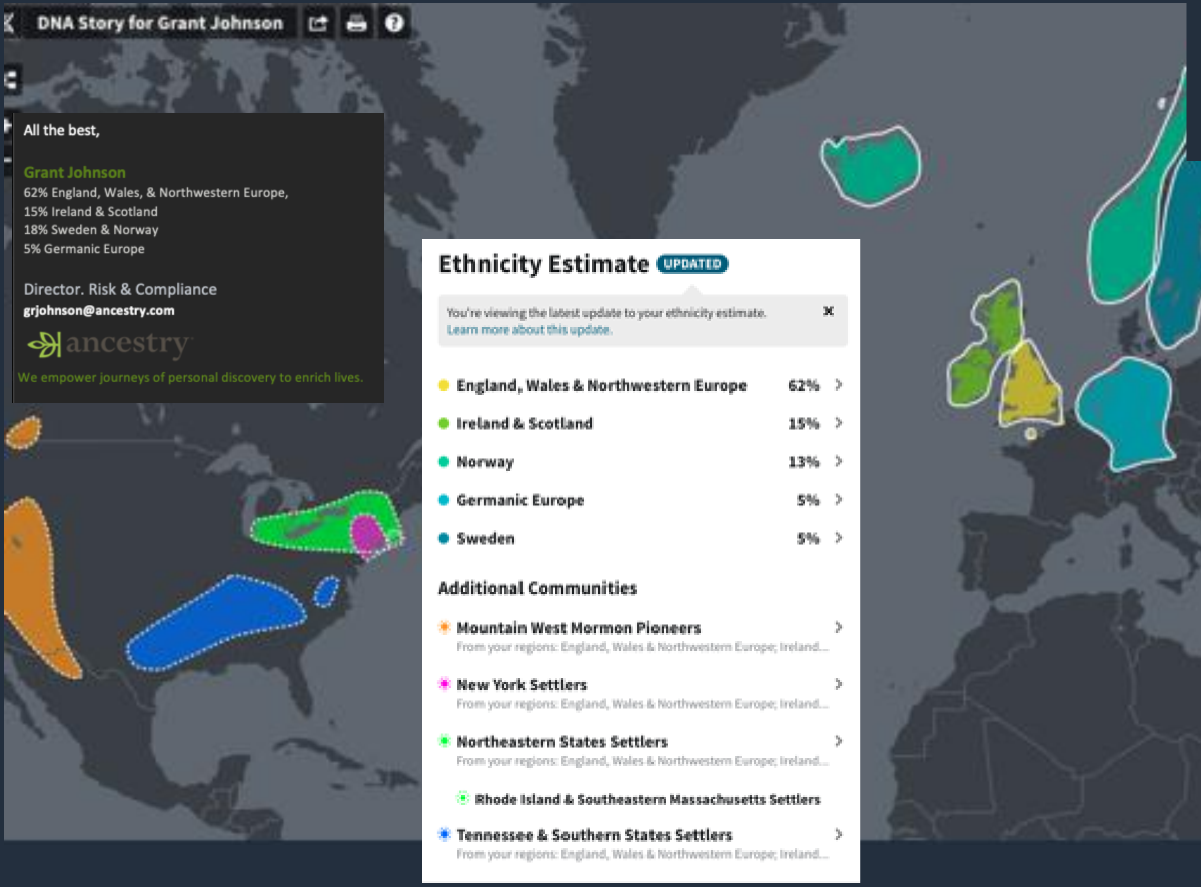
ancestry®

Fix it Once

How Ancestry Successfully Manages Vulnerabilities in the Cloud through Amazon Machine Images

INFOSEC
SECURING THE PAST, PRESENT AND FUTURE

Me…



DNA Story for Grant Johnson

All the best,

Grant Johnson
62% England, Wales, & Northwestern Europe,
15% Ireland & Scotland
18% Sweden & Norway
5% Germanic Europe

Director. Risk & Compliance
grjohnson@ancestry.com

ancestry

We empower journeys of personal discovery to enrich lives.

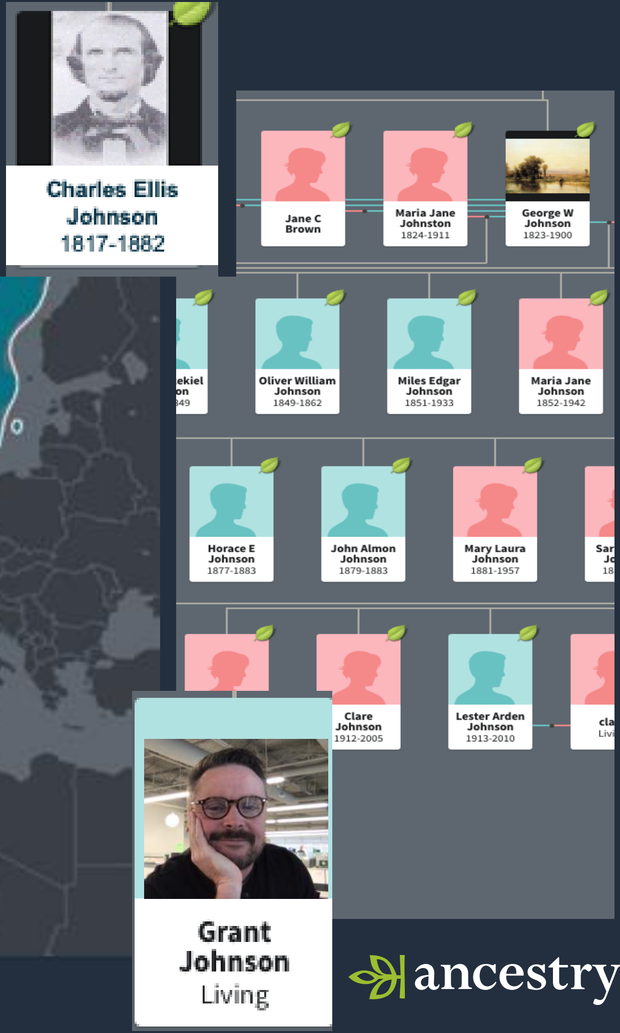
Ethnicity Estimate UPDATED

You're viewing the latest update to your ethnicity estimate.
Learn more about this update.

● England, Wales & Northwestern Europe	62%
● Ireland & Scotland	15%
● Norway	13%
● Germanic Europe	5%
● Sweden	5%

Additional Communities

- Mountain West Mormon Pioneers
  From your regions: England, Wales & Northwestern Europe; Ireland…
- New York Settlers
  From your regions: England, Wales & Northwestern Europe; Ireland…
- Northeastern States Settlers
  From your regions: England, Wales & Northwestern Europe; Ireland…
  - Rhode Island & Southeastern Massachusetts Settlers
- Tennessee & Southern States Settlers
  From your regions: England, Wales & Northwestern Europe; Ireland…



Charles Ellis Johnson
1817-1882

Jane C Brown

Maria Jane Johnston
1824-1911

George W Johnson
1823-1900

ekiel
on
349

Oliver William Johnson
1849-1862

Miles Edgar Johnson
1851-1933

Maria Jane Johnson
1852-1942

Horace E Johnson
1877-1883

John Almon Johnson
1879-1883

Mary Laura Johnson
1881-1957

Sar
Jo
18

Clare Johnson
1912-2005

Lester Arden Johnson
1913-2010

cla
Livi

Grant Johnson
Living

ancestry

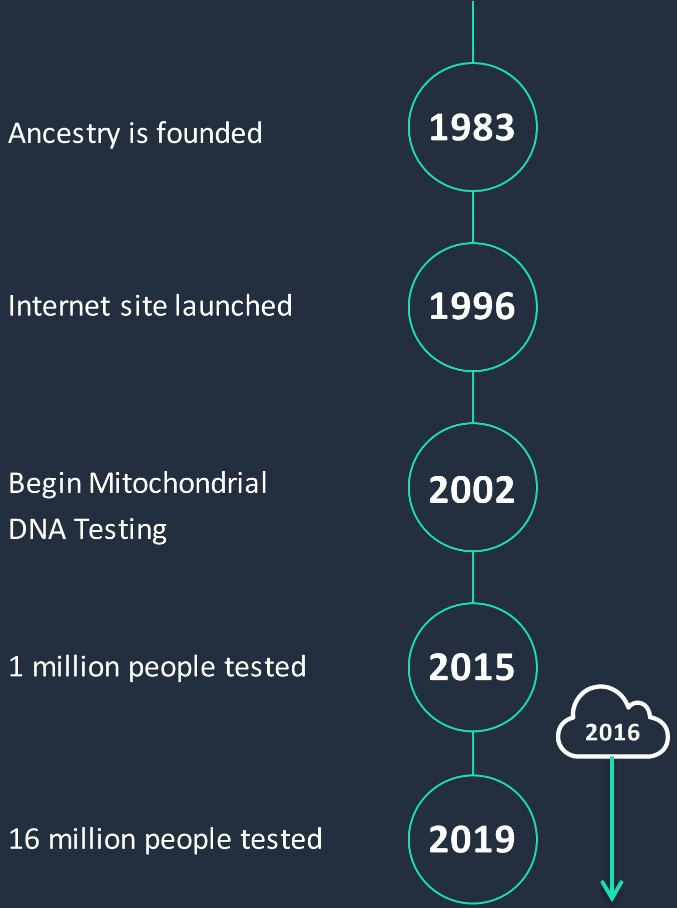
About us

We’re a science and technology company with a very human mission

- World’s largest online collection of family history records - billions & billions
- 3+ million wonderful subscribers
- 100 million family trees
- 10 web properties
- 3 petabytes of data under management

About us

- DNA kits available in 30+ countries
- 700K genomic markers
- 350 global regions
- Largest DNA repository in the world



Ancestry is founded	1983
Internet site launched	1996
Begin Mitochondrial DNA Testing	2002
1 million people tested	2015
16 million people tested	2019

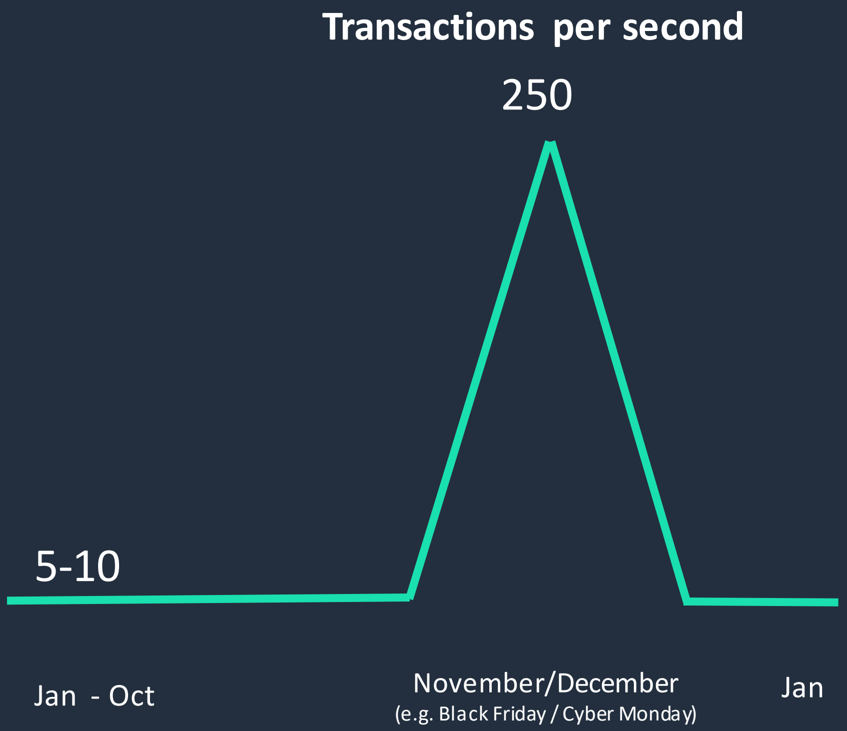
2016

ancestry

Challenges

Background: Why the Cloud?

- Growth
- Rapid cycle expansion
  - Fast moving, traffic & business cycles
- Resiliency & uptime
  - Multiple global regions
  - Multiple Availability Zones



ancestry

Tactical Approach to the Cloud

Each stack had to be imaged & rapidly deployable

- Needed to realized resiliency goals – ***Can't just lift-and-shift***
- Make use of cloud elasticity and containerization
- More Standardized toolset….

We use and mandate AWS Tags

- Every system needed a NAMED owner or was shutdown

Removed Access

- Separate AWS accounts for Development, Smoke, Production, SOX, and PCI
- Absolutely NO Dev Production Access Results: Huge ↓ P1 Incidents!
- **IF it is awake, it is subject to scanning**
- **Approved Images (AMI) with Authentication Keys**

Challenges

Each stack had to be imaged & rapidly deployable

- Needed to realize resiliency goals – Can’t just lift-and-shift
- Make use of cloud elasticity and containerization
- More standardized toolset

Here is what we did…

- Separate AWS accounts for Development, Smoke, Production, SOX, and PCI
- Absolutely NO Stage or Production access

  Spoiler alert: Huge ↓ P1 incidents!
- IF it is awake, it is subject to scanning
- Approved Images (AMI) with Authentication Keys
- Every system needed a NAMED owner or was shutdown (Qualys to find unnamed servers)

Solution

Approved Images – AMI’s

Ancestry required a new way of thinking about servers

Servers are cattle

Not pets

ancestry

Solution

Don’t push patches...patch the AMI

Shut down the old one

Spin up the new one with the new AMI

NO cows were harmed in our AWS migration!

Why Ancestry chooses AWS and Qualys

Why AWS?

- System resiliency
- Rapid elastic expansion
- Supported our rapid growth

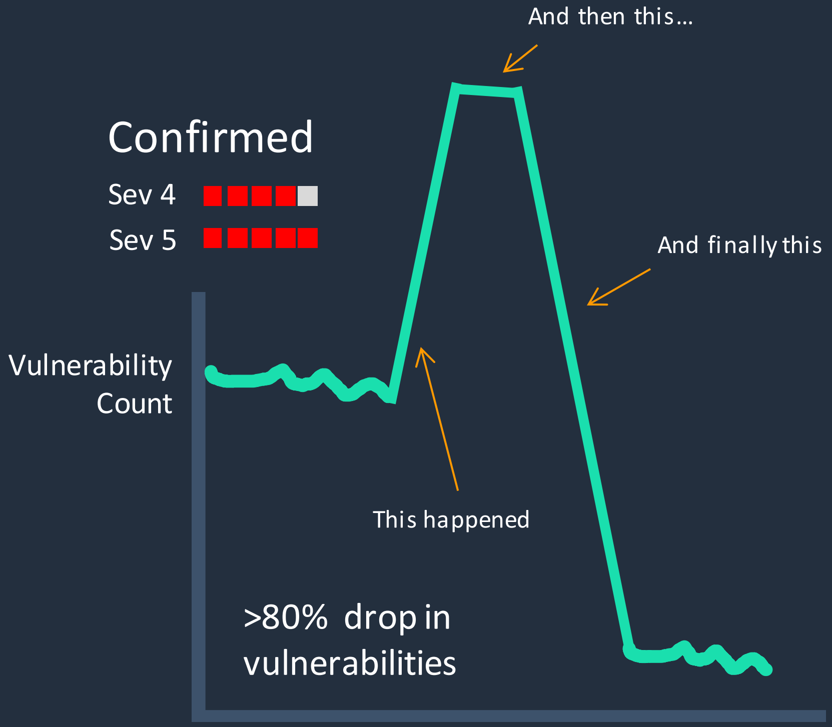
Why Qualys?

- Proven ability to work well with AWS – expanded with our needs
- Virtually maintenance free, once we set up
- The data was accurate – no false positives

Challenges

Lessons learned

- Don’t get fixated on the count of vulnerabilities
- Buy-in at executive level
- Think operationally – not exceptionally
- KEEP CALM and STICK to the process … it takes time to work
- Communication and visibility

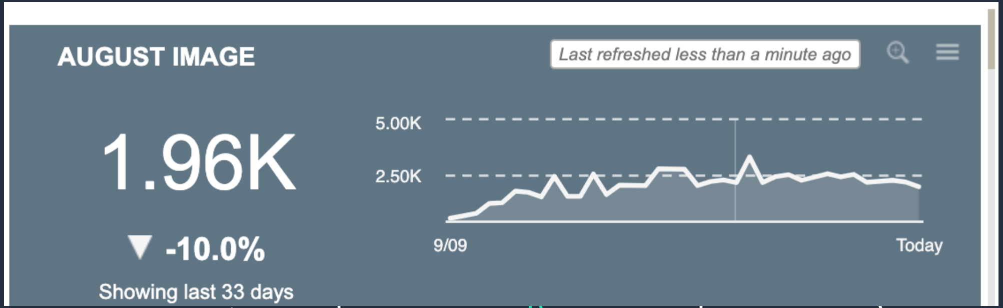


>80% drop in vulnerabilities

Don’t shoot for ZERO

Benefits are awesome

- My ask of Development:
  Do one thing. Update the image.
- Forced us to have a more homogeneous platform and process
- Synced security with business goals
- Process seems to be sustainable!
- 76%+ NIX scan are fully authenticated – 99% Windows
- Works for some applications as well



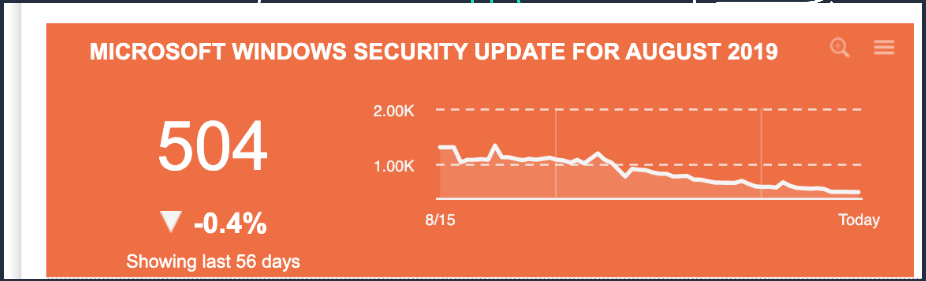
AUGUST IMAGE

Last refreshed less than a minute ago

1.96K

▼ -10.0%

Showing last 33 days



MICROSOFT WINDOWS SECURITY UPDATE FOR AUGUST 2019

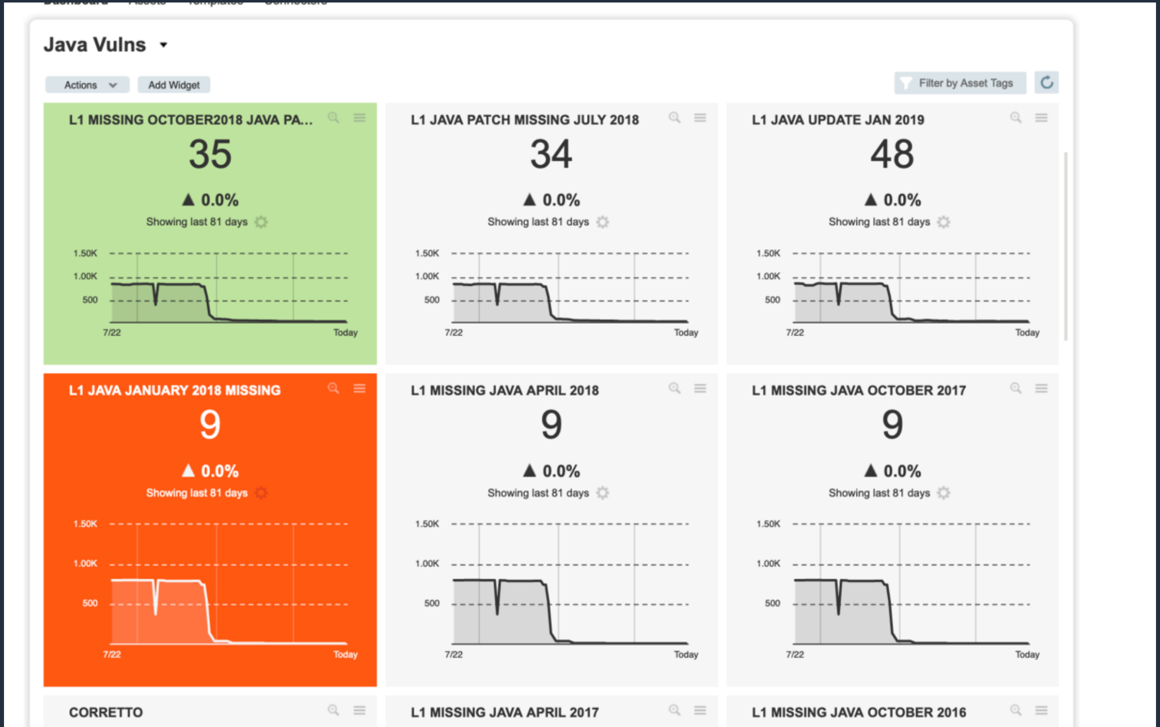
504

▼ -0.4%

Showing last 56 days

Benefits are awesome

- Works at the application layer as well



L1 MISSING OCTOBER2018 JAVA PA...
35
▲ 0.0%
Showing last 81 days

L1 JAVA PATCH MISSING JULY 2018
34
▲ 0.0%
Showing last 81 days

L1 JAVA UPDATE JAN 2019
48
▲ 0.0%
Showing last 81 days

L1 JAVA JANUARY 2018 MISSING
9
▲ 0.0%
Showing last 81 days

L1 MISSING JAVA APRIL 2018
9
▲ 0.0%
Showing last 81 days

L1 MISSING JAVA OCTOBER 2017
9
▲ 0.0%
Showing last 81 days

CORRETTO

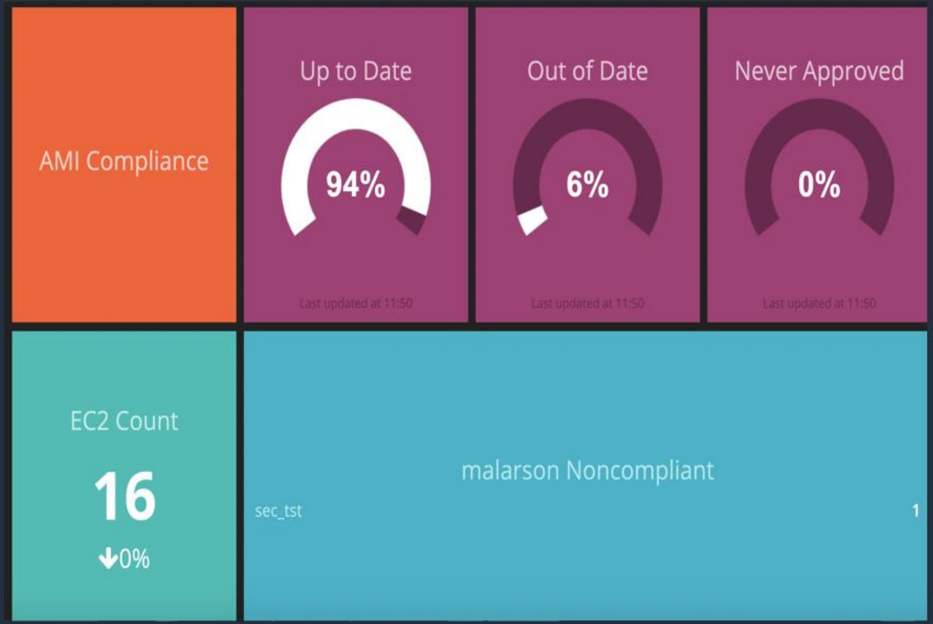
L1 MISSING JAVA APRIL 2017

L1 MISSING JAVA OCTOBER 2016

Dashboards

Key Metrics

- Use of approved image
- Confirmed 4s & 5s Ageing*
- Number of Vulns Fixed
- Scan coverage - Target 95%
- Authentication Percentage – Target 95%
- Vulnerabilities not fixed by Image



AMI Compliance

Up to Date
94%
Last updated at 11:50

Out of Date
6%
Last updated at 11:50

Never Approved
0%
Last updated at 11:50

EC2 Count
16
↓0%

malarson Noncompliant

sec_tst 1

* Aged based on vulnerability release date – pending…

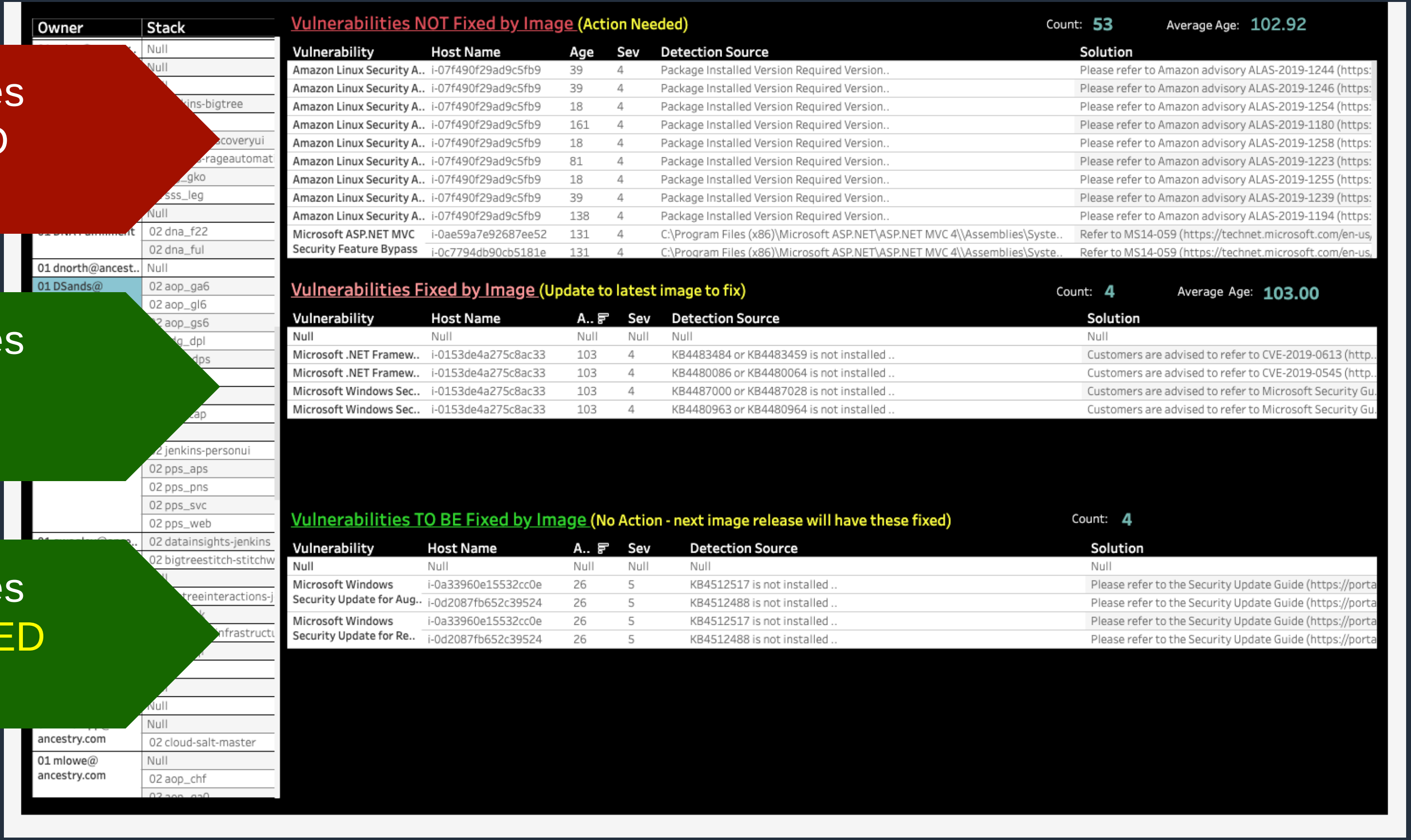
ancestry

Dashboards

Vulnerabilities
NOT FIXED
By Image

Vulnerabilities
FIXED
By Image

Vulnerabilities
WILL BE FIXED
By Image



Owner	Stack
	Null
	Null
	kins-bigtree
	coveryui
	-rageautomat
	_gko
	sss_leg
	Null
	02 dna_f22
	02 dna_ful
01 dnorth@ancest..	Null
01 DSands@	02 aop_ga6
	02 aop_gl6
	2 aop_gs6
	g_dpl
	dps
	ap
	2 jenkins-personui
	02 pps_aps
	02 pps_pns
	02 pps_svc
	02 pps_web
	02 datainsights-jenkins
	02 bigtreestitch-stitchw
	treeinteractions-j
	nfrastructu
	Null
ancestry.com	Null
	02 cloud-salt-master
01 mlowe@ ancestry.com	Null
	02 aop_chf

Vulnerabilities NOT Fixed by Image (Action Needed)

Count: 53 Average Age: 102.92

Vulnerability	Host Name	Age	Sev	Detection Source	Solution
Amazon Linux Security A..	i-07f490f29ad9c5fb9	39	4	Package Installed Version Required Version..	Please refer to Amazon advisory ALAS-2019-1244 (https:
Amazon Linux Security A..	i-07f490f29ad9c5fb9	39	4	Package Installed Version Required Version..	Please refer to Amazon advisory ALAS-2019-1246 (https:
Amazon Linux Security A..	i-07f490f29ad9c5fb9	18	4	Package Installed Version Required Version..	Please refer to Amazon advisory ALAS-2019-1254 (https:
Amazon Linux Security A..	i-07f490f29ad9c5fb9	161	4	Package Installed Version Required Version..	Please refer to Amazon advisory ALAS-2019-1180 (https:
Amazon Linux Security A..	i-07f490f29ad9c5fb9	18	4	Package Installed Version Required Version..	Please refer to Amazon advisory ALAS-2019-1258 (https:
Amazon Linux Security A..	i-07f490f29ad9c5fb9	81	4	Package Installed Version Required Version..	Please refer to Amazon advisory ALAS-2019-1223 (https:
Amazon Linux Security A..	i-07f490f29ad9c5fb9	18	4	Package Installed Version Required Version..	Please refer to Amazon advisory ALAS-2019-1255 (https:
Amazon Linux Security A..	i-07f490f29ad9c5fb9	39	4	Package Installed Version Required Version..	Please refer to Amazon advisory ALAS-2019-1239 (https:
Amazon Linux Security A..	i-07f490f29ad9c5fb9	138	4	Package Installed Version Required Version..	Please refer to Amazon advisory ALAS-2019-1194 (https:
Microsoft ASP.NET MVC Security Feature Bypass	i-0ae59a7e92687ee52	131	4	C:\Program Files (x86)\Microsoft ASP.NET\ASP.NET MVC 4\\Assemblies\Syste..	Refer to MS14-059 (https://technet.microsoft.com/en-us,
	i-0c7794db90cb5181e	131	4	C:\Program Files (x86)\Microsoft ASP.NET\ASP.NET MVC 4\\Assemblies\Syste..	Refer to MS14-059 (https://technet.microsoft.com/en-us,

Vulnerabilities Fixed by Image (Update to latest image to fix)

Count: 4 Average Age: 103.00

Vulnerability	Host Name	A..	Sev	Detection Source	Solution
Null	Null	Null	Null	Null	Null
Microsoft .NET Framew..	i-0153de4a275c8ac33	103	4	KB4483484 or KB4483459 is not installed ..	Customers are advised to refer to CVE-2019-0613 (http..
Microsoft .NET Framew..	i-0153de4a275c8ac33	103	4	KB4480086 or KB4480064 is not installed ..	Customers are advised to refer to CVE-2019-0545 (http..
Microsoft Windows Sec..	i-0153de4a275c8ac33	103	4	KB4487000 or KB4487028 is not installed ..	Customers are advised to refer to Microsoft Security Gu..
Microsoft Windows Sec..	i-0153de4a275c8ac33	103	4	KB4480963 or KB4480964 is not installed ..	Customers are advised to refer to Microsoft Security Gu..

Vulnerabilities TO BE Fixed by Image (No Action - next image release will have these fixed)

Count: 4

Vulnerability	Host Name	A..	Sev	Detection Source	Solution
Null	Null	Null	Null	Null	Null
Microsoft Windows Security Update for Aug..	i-0a33960e15532cc0e	26	5	KB4512517 is not installed ..	Please refer to the Security Update Guide (https://porta
	i-0d2087fb652c39524	26	5	KB4512488 is not installed ..	Please refer to the Security Update Guide (https://porta
Microsoft Windows Security Update for Re..	i-0a33960e15532cc0e	26	5	KB4512517 is not installed ..	Please refer to the Security Update Guide (https://porta
	i-0d2087fb652c39524	26	5	KB4512488 is not installed ..	Please refer to the Security Update Guide (https://porta

ancestry

Q&A

INFOSEC
SECURING THE PAST, PRESENT AND FUTURE

Thank you!

ancestry